"It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices

Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou[†], Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, Florian Schaub[†]
Carnegie Mellon University & [†]University of Michigan
{htq, spearman, jiaminw, acquisti, lorrie, ns1i}@andrew.cmu.edu
{yixinz, fschaub}@umich.edu

ABSTRACT
We conducted an in-lab user study with 24 participants to explore the usefulness and usability of privacy choices offered by websites. Participants were asked to find and use choices related to email marketing, targeted advertising, or data deletion on a set of nine websites that differed in terms of where and how these choices were presented. They struggled with several aspects of the interaction, such as selecting the correct page from a site's navigation menu and understanding what information to include in written opt-out requests. Participants found mechanisms located in account settings pages easier to use than options contained in privacy policies, but many still consulted help pages or sent email to request assistance. Our findings indicate that, despite their prevalence, privacy choices like those examined in this study are difficult for consumers to exercise in practice. We provide design and policy recommendations for making these website opt-out and deletion choices more useful and usable for consumers.

Author Keywords
Privacy; usability; privacy controls; email marketing; targeted advertising; data deletion.

CCS Concepts
•**Security and privacy** → **Usability in security and privacy;** *Privacy protections;* •**Human-centered computing** → **Empirical studies in HCI;** *Empirical studies in interaction design;* •**Social and professional topics** → *Privacy policies;*

INTRODUCTION
An expanding body of privacy regulations requires websites and online services to present users with notices and choices regarding the usage of their data. These regulations aim to provide transparency about data processing policies and give users access and control over their own data. Some regulations — such as the General Data Protection Regulation (GDPR) and a few US laws — include specific usability requirements [3, 7, 40]. In part due to these regulations, privacy choices now seem to be ubiquitous on websites. Particularly common are opt-outs for email communications or targeted ads, options for data deletion, and controls and consent for use of cookies [15].

However, availability does not imply usability, leaving open the question of whether these controls are actually useful to consumers. We contribute a holistic usability evaluation of the end-to-end interaction required to use common implementations of these privacy choices. Past work has found various usability problems with such controls, particularly in tools for limiting targeted advertising (e.g., [12, 21]). We expand on that work by exploring the usability of websites' own opt-outs for targeted ads. Furthermore, we examine choices beyond those related to advertising, providing insight into the usability of email marketing and data deletion choices required by the CAN-SPAM Act and GDPR, respectively.

We conducted an in-lab usability study with 24 participants. Participants were first asked about their expectations regarding websites' data practices and privacy controls. They completed two tasks that were representative of common practices for offering privacy choices, as identified by prior work [15]. Tasks differed by the choice type (opting out of email communication, opting out of targeted ads, or requesting data deletion), choice location (account settings, privacy policy), and mechanism type (described in policy text, link from policy text).

We find that despite general awareness of deletion mechanisms and opt-outs for advertising and email, participants were skeptical of the effectiveness of controls provided by websites. On the nine websites studied, participants struggled most with discovering and recognizing pages with opt-out information and resorted to consulting help pages or contacting the website. Participants also expressed desire for additional controls over data sharing and deletion. Our findings suggest several implications applicable to websites similar to those in this study for making these online opt-out and deletion choices more usable and useful to consumers.

BACKGROUND & RELATED WORK
We first summarize legislation and self-regulatory industry guidelines relevant to controls for email marketing, targeted advertising, and data deletion. We then discuss prior studies on the usability of privacy controls.

CHI '20, April 25–30, 2020, Honolulu, HI, USA.

ACM ISBN 978-1-4503-6708-0/20/04.
http://dx.doi.org/10.1145/3313831.3376511

Regulatory Background

The European Union's General Data Protection Regulation (GDPR) requires websites to provide several types of privacy choices for European consumers and places a special emphasis on the usability of these choices. Relevant user rights under the GDPR include the "right to object" (Art. 21) to the use of data for direct marketing purposes and the requirement for clear affirmative consent to targeted advertising (Art. 4). Such consent in practice is often implemented by cookie consent banners [4]. Moreover, the GDPR grants a "right to be forgotten," allowing consumers to request data processors to delete their personal data (Art. 17) [8].

While the United States does not have a single comprehensive privacy law, several sectoral laws pertain to the privacy controls we examined in our study. The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act requires companies to comply with consumers' wishes to opt out of receiving marketing emails, and provide a clear explanation for how to use the opt-out [10]. Other laws only apply to specific populations. For example, the Children's Online Privacy Protection Act of 1998 (COPPA) requires companies that collect data from children under 13 to honor parental requests to stop further data collection and delete already-collected data [11]. Effective in 2020, the California Consumer Privacy Act (CCPA) provides California residents rights to opt out of sales of their personal data for marketing purposes and, under certain circumstances, request deletion [3, 28].

Advertising industry organizations such as the Network Advertising Initiative (NAI), Digital Advertising Alliance (DAA), and Interactive Advertising Bureau Europe (IAB Europe) have adopted self-regulatory requirements for their online advertising practices [5, 17, 30]. Specifically, members of the DAA must provide consumers the choice to opt out of tracking-based targeted advertising [5]. In light of recent GDPR requirements, the IAB Europe also developed new guidelines for member advertisers related to transparency and consent [18].

Design of Privacy Choices

An empirical analysis of controls for email marketing, targeted advertising, and data deletion conducted by Habib et al. found that privacy choices are often presented through websites' user account settings and privacy policies. However, the terminology used in privacy policies to present these choices is inconsistent across websites, and quite often choices are not adequately described [15]. This has negative usability implications, as privacy policies still suffer from poor readability and consumers rarely read them [9]. Further exasperating this usability issue is the potential use of dark patterns and default settings, which could nudge users away from more privacy protective options [1, 13, 34, 43]. Gray et al. found that users are more likely to agree to the default option because of a belief that the product has their best interest in mind, which may not be the case with respect to data practices and privacy and could lead to unintended consequences [14].

While the goal of the GDPR is to empower consumers to have greater control over their personal data, Sanchez-Rola et al. found that numerous websites in the sample they analyzed presented misleading information about choices, and few websites provided opt-outs for ad tracking that were easy to find or effective [37]. The GDPR also led to an increase in the display of cookie consent banners, but common implementations suffer from functional and usability issues [4]. Utz et al. found that consumers often clicked cookie consents out of habit, or believed that the website would not work absent a click on the consent box [42]. On the other hand, with the implementation of the GDPR, there is also some evidence that companies are shifting towards better practices. A study by Linden et al. suggests that the GDPR was a major driving force towards significant improvements in the presentation of privacy policies inside and outside of the EU [22].

Our study expands upon this prior work by examining user expectations for privacy choices and evaluating current practices for offering choices against these expectations. It highlights additional usability issues with the design of privacy choices that make them difficult for people to use and understand.

Usability of Privacy Choices

We next present prior work examining the usability of the privacy choices that were the focus of this study: email marketing, targeted advertising, and data deletion.

Email Marketing Opt-Outs

In addition to the risk of legal penalties, businesses may also risk losing customers by using poor practices in email unsubscribe processes. Results from a study of marketing unsubscribe choices by the Nielsen-Norman group indicate that users may become annoyed with companies and report legitimate messages as spam if unsubscribe options are not clear. They recommend making unsubscribe links easy to notice and click or tap on a mobile device. They also suggest removing unnecessary feedback steps or confirmation messages and avoiding confusing checkboxes on unsubscribe pages [31].

The Internet Society's Online Trust Alliance (OTA) conducted an audit of 200 North American online retailers to assess compliance with best practices for email sign-up and unsubscribe experiences. While the vast majority of audited retailers had adopted best practices, the report highlighted room for improvement, particularly related to the visibility of opt-out links in emails. While 84% of retailer emails had clear and conspicuous unsubscribe links, a third presented the link in a smaller than recommended font size. Additionally, 29% of retailers had unsubscribe text that did not meet minimum W3C guidelines for contrast ratios, and 64% of retailers did not meet W3C's enhanced guidelines [35].

Our study provides additional insight into the usability of email opt-outs through an empirical user study and evaluates email controls other than unsubscribe links, such as those offered through account settings and privacy policies.

Targeted Advertising Opt-Outs

Prior work has shown that websites are non-compliant with self-regulatory guidelines for targeted advertising, resulting in limited transparency in opt-out choices for users [16, 20]. Opt-out tools developed by the advertising industry have also been found to be misunderstood by users. Ur et al. showed

that the DAA's AdChoices icon does not clearly communicate whether or not an ad is targeted [41]. Additionally, NAI's opt-out tool led users to believe incorrectly that they were opting out of all data collection [26]. Furthermore, these opt-out tools rely on cookies, which can cause additional issues for users. For example, when users clear their cookies their opt-out preferences will also be removed in the process, which would require them to opt out again [25].

Browser extensions that block advertising trackers only partially resolve some of these issues. Studies have found that internet users download blocking extensions for a better browsing experience but still retain a limited understanding of online tracking [24, 38]. Pujol et al. found that many users use ad-blockers with default settings, which for some extensions might not actually block all web trackers [36]. This suggests that even with blocking extensions, people are not fully aware of the ad opt-out choices they can exercise online. While users state they want more control over tracking, they are reluctant to engage deeply with respective tools [27, 39].

Prior research has largely evaluated controls for targeted advertising on the basis of compliance with industry guidelines and users' perceptions of what they do, but has not holistically examined the end-to-end interaction required to use them. Our study provides additional insights by looking more deeply into how users discover targeted advertising controls, in the context of how they are commonly presented on websites.

Data Deletion Choices

Few studies have evaluated data deletion mechanisms, and thus there are few guidelines or best practices. Murillo et al.'s 2018 qualitative study examined user understanding of online data deletion and expiration. They found that most participants were aware of a "backend" to the data deletion process (versus having an understanding completely based on user interface components such as delete buttons and trash icons), and they suggested that information about data deletion should use this understanding to explain technical constraints of data deletion and to help users understand data retention periods. They also found that participants preferred to have context-dependent control over the expiration of their data, rather than just having a fixed chronological expiration period [29].

Recent evidence indicates that the GDPR has lead to increased availability of deletion controls, which are often provided as instructions through a website's privacy policy for requesting deletion of personal data [13, 15]. The service JustDelete.me provides a database with ratings of the ease of deleting data from over 500 different websites, and compiles direct links to the deletion options on those sites. Nearly 40% of the websites listed in the database are rated as having "hard" or "impossible" deletion processes. However, this database does not provide analyses of the full user interaction required to delete data, nor does it publish its methodology for determining these ratings or suggest best practices for deletion interfaces [19].

In 2019, Habib et al. analyzed 150 English-language websites to assess the usability and interaction paths of data deletion mechanisms (as well as email and advertising opt-out mechanisms). While 74% of websites in their sample offered deletion controls, only 27 included a direct link to a tool or request form; 81 offered instructions for a data deletion request rather than providing a simple tool or form. The types of deletion and expiration options were not consistent from website to website, and the time frame in which data deletion would occur was often ambiguous. Many actions, including form fields and extraneous confirmations, were sometimes required in order to delete data. For example, 38 user actions — including filling out a form with 22 checkboxes — were required to request data deletion from the New York Times [15].

While prior work has studied users' mental models of data deletion through interviews [29], prior usability evaluations of deletion controls have relied on analysis by usability experts [15, 19]. Our study builds on this work with a user study that confirms reported usability issues and uncovers others.

STUDY DESIGN

We conducted a lab study with 24 participants. In this section we describe our study design and data analysis approach.

Study Session Components

Each lab session consisted of an interview portion followed by a set of tasks conducted on a lab computer. Participants were also asked follow-up questions after completing each task.

Interview

The first portion of the study session, a semi-structured interview, had a median length of 11 minutes (min: 5 minutes, max: 22 minutes). First, we asked participants what types of data they thought websites collected about them and how they thought it was used. Next we asked participants what types of controls they expected to have over how websites could use their data, as well as where they expected to be able to find these controls. To learn more about expectations related to email marketing, targeted advertising, and data deletion specifically, we asked participants to recall a recent time when they received a marketing email, saw a targeted ad, and provided a website with personal information. For each, we followed up with questions about what types of control they thought were available, and how they would attempt to exercise that control.

Task Selection

In the second portion of the study session, we asked each participant to complete two opt-out tasks on a lab computer. In each task, participants were asked to use a privacy choice on a website while thinking aloud. Each privacy choice task was one of the following: opting out of email newsletters from a website, opting out of targeted advertising on a website, or requesting deletion of personal information from a website. Although other privacy choices exist, we wanted to examine the usability of a set of choices over different types of data handling practices. Additionally, the choices selected are prevalent in the current online ecosystem and fall under legal or other regulatory requirements.

In prior work, we reviewed controls for email marketing, targeted advertising, and data deletion on 150 websites and found that these choices are most commonly presented using one of three patterns: a user account setting, a link from the privacy policy, or text instructions in the privacy policy [15]. To

Website Name	Task Type	PP | AS	# Actions	Mechanism
majorgeeks.com	email	AS	9	checkbox
foodandwine.com	email	PP	5	link to email options
internshala.com	email	PP	9	text, refer to emails
wordpress.com	ads	AS	9	toggle option
colorado.edu	ads	PP	16	links to opt-out tools
coinmarketcap.com	ads	PP	10	text, delete cookies
phys.org	deletion	AS	9	delete account
nytimes.com	deletion	PP	46	link to request form
runescape.com	deletion	PP	9	text, email request

Table 1. The websites used for email opt-out, targeted advertising opt-out, and date deletion tasks and their associated mechanisms in the privacy policy (PP) and account settings (AS), as well as the minimum number of user actions required to exercise each control.

identify specific tasks for this user study, we examined the collected empirical data and looked for websites that used just one of the three patterns (some websites used more than one pattern, e.g., both a user account setting and privacy policy link). For each of the *task types*, we selected three websites that followed these patterns, resulting in a set of nine websites. The websites selected and their choice mechanisms in the privacy policy or user account settings are presented in Table 1.

To minimize learning effects and prevent fatigue, we counterbalanced and stratified tasks such that each participant completed two different task types. One task was selected to be on a website with an account settings mechanism and the other task on a website with a privacy policy mechanism, allowing us to examine the usability of the most common practices used by websites. This resulted in 12 possible groupings of the websites selected for the study. We recruited 24 participants and assigned a pair of participants to each grouping, with each member of the pair performing the tasks in the inverse order.

Task Introduction

Prior to each study session, researchers opened a new window in Google Chrome's Incognito mode and logged into a Gmail account created for the study. Before being given their first task, participants were told that they could use this Gmail account and could search online for any information that they needed to complete the task. Participants were also notified that, if applicable, they could assume they had user accounts on the websites they would visit for the study tasks. Participants were not required to use their own credentials or personal information for any of the tasks, and instead were provided with credentials created for the study through printed index cards when reaching the log-in step on the website.

We described the email opt-out, targeted advertising opt-out, and deletion tasks to participants as the following scenarios:

> You just got the tenth update email from [website] today, and now you want to stop receiving them.
>
> You've been seeing advertisements on [website] for a pair of shoes that you searched for last month, and now you want to stop seeing them.
>
> You're uncomfortable with [website] keeping a record of your location, and want to remove all of your data from the company's databases.

After being read the appropriate scenario, participants were instructed to open a new browser tab or proceed as they would at home while thinking aloud.

Task Follow-Up

After each task, we asked a set of follow-up questions regarding the participant's experience with the task and their understanding of what effects their actions would have. We also asked about their past experiences with similar tasks and their familiarity with the website used in the task.

After participants completed both tasks and the task follow-up questions, we asked them which task they found easier, and why. We also asked about their past choices to use opt-out mechanisms or privacy controls on websites. Lastly, we inquired as to whether they wished websites offered any additional controls related to privacy or personal data and what they thought they should look like.

Data Collection

One researcher moderated all participant sessions. A second researcher attended each session to take notes. At the beginning of their session, participants completed a consent form that described the nature of the interview and tasks and notified participants that audio and screen recordings would be captured. We audio-recorded participants' responses to interview questions, comments and questions during the computer tasks, and responses to follow-up questions after the computer tasks. Participants' actions during the computer tasks were screen-recorded. This study was approved by the Institutional Review Boards (IRB) at Carnegie Mellon University and the University of Michigan.

The 24 participants were recruited locally in Pittsburgh, Pennsylvania using Craigslist, Reddit, and a university subject pool. In recruitment posts, potential participants were invited to complete a screening survey with questions about demographics, as well as engagement in four common privacy practices selected from a Pew Research Center survey [23]. A sample of participants — diverse in gender, age, and educational attainment — was selected from among the respondents. Those who completed the in-lab study session were compensated with a $20 Amazon gift credit. The study sessions lasted a median of 50 minutes (min: 30 minutes, max: 78 minutes). The large variance in session duration was related to how fast participants were able to complete their tasks. While all participants attempted their tasks, those who stated they did not know what to do next or still had not completed the task after eight minutes were given a hint to log in or look for a "privacy-related page" (depending on the task). This threshold of eight minutes was determined through pilot sessions. Any assistance provided was noted and incorporated into our analysis.

Data Analysis

Interview recordings were transcribed using an automated transcription service (temi.com), and a researcher then corrected errors in the transcripts. The use of a third-party transcription service was IRB-approved, and participants consented to the sharing of recordings with a third-party service. We took extra measures to preserve participants' privacy prior to uploading the recordings by removing any personally identifying

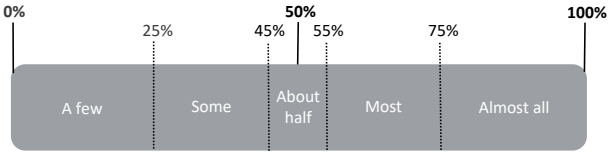

Figure 1. Terminology used to present relative frequency of themes.

details, such as name and address, that a small number of our participants revealed during their interview. We conducted inductive coding on the interview transcripts. To develop an initial codebook, one researcher performed open coding to identify themes and merged common codes as needed. Two researchers then collaboratively revised the codebook after individually coding a random sample of six interviews using the initial iteration of the codebook and reviewing all disagreements in their coding. After coming to an agreement on the codebook, the remainder of the interviews were double-coded. Any disagreements were again reviewed and reconciled.

We created an analysis template to systematically count the interactions and errors made during the tasks. One researcher reviewed all screen recordings of the session tasks along with any researcher notes from the session to create initial counts of interactions and errors. Another researcher then reviewed and confirmed the interactions recorded.

We organized our findings according to the User Action Framework, which offers a systematic framework for assessing and reporting usability data. Within this framework, Andre et al. [2] adapted Norman's theory of human-computer interaction [32] and discuss user interaction in terms of four cyclic phases: high-level planning ("users determine what to do"), translation ("users determine how to do it"), physical action ("users do the physical actions they planned"), and assessment ("users assess the outcome of their actions"). We previously applied this framework to online privacy choices in our empirical analysis of opt-out and data deletion actions across websites, and mapped these phases of the interaction to *finding*, *learning*, *using*, and *understanding* privacy choice mechanisms [15]. Here we apply the same framework to the actions we observed in the lab.

As our study was primarily qualitative, we do not report exact numbers when presenting most of our study findings. However, following recent qualitative work at CHI [6], we adopted the terminology presented in Figure 1 to provide a relative sense of frequency of major themes.

Limitations

The exploratory nature of this study provides insights into possible usability issues with common practices used to provide privacy choices, but cannot provide quantitative claims about how frequently these issues may occur in the real world. Similarly, our limited sample size of 24 participants, though diverse, was not representative of all internet users, and likely over-represented technically savvy users. Thus the frequency of issues reported by our participants may not reflect the frequency with which these issues would be encountered by a general population. However, it is unlikely that less technically savvy users would face fewer issues when opting out or deleting their data. As such, the issues and opinions highlighted only represent a subset of all possible ones.

While our sample of nine websites was representative of the common practices websites use to provide privacy choices, it is not representative of all types or categories of websites that exist. Our results may not generalize to other types of websites, particularly those that are more complex than those included in our sample and offer multiple products or services. Additionally, design variations and specific peculiarities of each website may have impacted the difficulty of exercising the privacy choices present and thus participants' opinions. However, this was a deliberate trade-off as using live websites allowed us to gain insight into the usability of real-world privacy choices. We note specific features that seemed particularly detrimental or helpful when exercising privacy controls.

While our study was designed to mitigate learning effects, it is still possible that participants used knowledge acquired in their first task to complete their second task. Similarly, while we avoided directly mentioning "privacy" or "security" during the pre-task interview (unless a participant brought up the topic), the questions may have biased participants to think more about privacy and security than they otherwise would have.

PARTICIPANTS

Table 2 provides a summary of participant demographics, as well as which tasks participants were assigned. In our sample, 13 participants identified as female and 11 as male. Our sample had a wide distribution of ages, but skewed towards higher levels of educational attainment. Six participants reported having an education in or working in computer science, computer engineering, or IT. In their responses to the screening survey, all 24 participants reported to have cleared cookies or browsing history, 22 had refused to provide information about themselves that was not relevant to a transaction, 13 had used a search engine that does not keep track of search history, and 10 added a privacy-enhancing browser plugin like DoNotTrackMe or Privacy Badger. This distribution is somewhat higher than that found by Pew [23], suggesting our sample may be more privacy-aware than the general public. Almost all participants reported having prior experience with controls for email marketing, and most had prior experiences with advertising and deletion controls.

RESULTS

We next present our findings structured around the four stages of the interaction cycle: finding, learning, using, and understanding privacy choice mechanisms. We highlight participants' expectations, actual performance in session tasks, as well as website practices that make exercising privacy choices more difficult for users and those that make it easier.

Planning: Finding Privacy Choices

Participants expected to find privacy choices within the context of how a website uses their data (for example, unsubscribe links within emails) or on a user account settings page. The presence of multiple paths to a privacy control made the control easier to find.

ID	Gender	Age	Education	Technical	Task 1	Task 2
P1	F	35-44	Professional		majorgeeks	runescape
P2	F	18-24	Bachelors		wordpress	internshala
P3	F	25-34	Some college		wordpress	foodandwine
P4	M	55-64	Bachelors		wordpress	nytimes
P5	F	45-54	Bachelors		wordpress	runescape
P6	F	25-34	Masters		phys	internshala
P7	F	45-54	Associates		phys	foodandwine
P8	F	25-34	Bachelors		phys	coinmarketcap
P9	F	25-34	Bachelors		phys	colorado
P10	M	25-34	Masters	X	colorado	majorgeeks
P11	M	55-64	Masters		nytimes	majorgeeks
P12	F	18-24	Associates		internshala	wordpress
P13	M	35-44	Some college	X	foodandwine	wordpress
P14	F	18-24	Bachelors		nytimes	wordpress
P15	M	18-24	Bachelors		runescape	wordpress
P16	F	55-64	Bachelors	X	foodandwine	phys
P17	M	45-54	Associates	X	coinmarketcap	phys
P18	M	55-64	High school		colorado	phys
P19	F	55-64	Masters		majorgeeks	coinmarketcap
P20	M	35-44	Associates	X	majorgeeks	colorado
P21	F	35-44	Masters		majorgeeks	nytimes
P22	M	25-34	Bachelors		coinmarketcap	majorgeeks
P23	M	18-24	Masters		internshala	phys
P24	M	25-34	Bachelors	X	runescape	majorgeeks

Table 2. Participant demographics (gender, age, education, technical background) and task assignments.

Expectations are dependent on choice type

In response to pre-task questions, some participants mentioned expecting to find data-use controls in the account settings or on a privacy settings page. A few participants mentioned consent dialogues, either through the browser or the website. Additionally, a few participants described browser settings or functions, such as private browsing and plugins.

Participants had similar responses when describing where they would like privacy controls to be placed. Half of the participants suggested that controls should be placed within a website's account settings. Some preferred to see privacy controls in context on the website (e.g., where data is collected). Other suggestions provided by participants included being able to email a company with requests and receiving monthly digest emails summarizing the data the website has about them.

When asked about email marketing controls, almost all participants mentioned unsubscribe links within emails. Some also described more granular controls, such as the ability to select which marketing messages to receive or to change the frequency of emails through website account settings. Some described other control mechanisms, such as contacting the website and using unsubscribe features built into email clients.

To control the display of targeted advertising, about half the participants mentioned privacy enhancing strategies, such as using ad-blocking extensions, clearing the browser history, using private browsing mode, changing browser settings, or using a privacy-protective search engine. A few participants mentioned being able to find controls by interacting with the corner of an advertisement (likely referring to the DAA's AdChoices icon or ad controls provided by social media sites). Only a few participants mentioned controls for advertising being available in the account settings. A few also mentioned avoiding clicking on ads as a type of control.

Most participants expected deletion controls to be available in the account settings, and some believed that deletion could be achieved by contacting the website. Only a few participants mentioned finding deletion controls elsewhere on the website, such as in a frequently-asked-questions page.

Participants' initial strategies varied by choice type

Most of the 16 participants assigned to an email opt-out task first looked for or used an unsubscribe link in an email sent by the website, which could be found in the provided Gmail account. Almost all participants reported using such links prior to the study. A few had other initial strategies for finding unsubscribe mechanisms, such as using the search feature of the browser to find the term "unsubscribe" on the home page or the search feature of the website to find the privacy policy.

Participants used a variety of strategies for completing their targeted advertising opt-out task, some of which were more effective than others. Some first went to the account settings, while only a few first looked in the privacy policy. A few explained that they would try to find an ad on the website and look for an icon leading to opt-out options. A few went into the browser settings to look for advertising-related options, while a few others immediately resorted to emailing the website for help. As P18 reasoned, *"Well, if they're not able to help then they would respond back and say here is the correct way to opt out of what you're looking for."* A few participants looked for opt-out choices on other pages, such as the website's cookie policy, terms of service, and frequently-asked-questions page.

Participants had a more uniform set of strategies for deletion mechanisms. Most immediately logged into the website. A few resorted to frequently-asked-questions pages or contacting the website. Finally, a few participants looked for account-related information in registration emails from the website.

Policy and settings mechanisms required assistance

Almost all participants required assistance finding the account setting or privacy policy mechanism related to their study task. On the three websites that had privacy choices in account settings, some were able to use the mechanism on their own after being prompted to log into the website, but a few needed further guidance to look within the account settings to complete the task. P6, who was unable to find the advertising opt-out on **wordpress.com** described the process: *"It's what I call a scavenger hunt. I've gone all throughout this website, apparently a legitimate website, but I still can't do what I really like to do."* On the six websites where the privacy choices were in the privacy policy, some were able to find the privacy choice text or link without guidance (however P10 admitted they were prompted to think about privacy because of the pre-task interview). A few were able to use the choice mechanism after they were given the hint to look for a privacy-related page, while a few others did not initially see the control in the policy and required prompting to look further.

Poor labels cause confusion

On two of the websites, there were multiple pages that had labels with words that were related to what the task was. For example, some participants assigned to opt out of email marketing from **majorgeeks.com** went to a different settings page called "alert preferences" that included settings related to notifications received while on the website. The correct setting

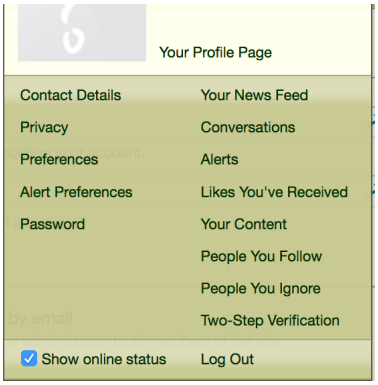

Figure 2. Screenshot of settings menu on `majorgeeks.com` where participants had difficulty finding the correct path to e-mail opt-outs.

could be found under the "privacy" or "contact details" settings pages. However, as seen in Figure 2, these options were presented in a list with no descriptions. Similar confusion occurred on `coinmarketcap.com` where a few participants assigned to find controls related to targeted advertising went to a page linked from the homepage called "advertisers" with information for companies that wished to place ads on the site. This suggests that more descriptive labels on these websites would help users find choice mechanisms more easily.

Multiple paths made choices easier to find

On some websites, there were multiple paths to the same choice mechanism, which made them easier to find. All participants assigned to request data deletion from `nytimes.com` first visited the account settings, where they found a link to the privacy policy, which in turn contained a link to the request form. Similarly, most participants assigned to request data deletion from `runescape.com` used the site's search feature or looked through its support pages and found a page titled "Your Personal Data Rights," which provided a summary of the same information provided in the privacy policy. However, one additional location where participants expected an opt-out choice for email marketing was on the page to subscribe to emails. All four participants assigned to find the opt-out link in `foodandwine.com`'s privacy policy clicked on the prominent "subscribe" button on the homepage and expected to find a means to unsubscribe.

Translation: Learning Privacy Choices

Participants had clear expectations about what choices available to them should do. We also observed several design decisions made by websites that impacted participants' comprehension of these choices.

Participants desired controls over data sharing and deletion

Participants demonstrated incomplete mental models of the choices that were provided to them, especially when describing controls related to how websites can use collected data in the abstract. The only website-offered controls that were mentioned by multiple participants were cookie consent notices and security controls, such as encryption or multi-factor authentication. A few participants mentioned withholding information about themselves when using a website or avoiding using a website entirely. However, a few participants discussed deletion controls prior to being prompted.

Participants' understanding of website-provided controls appeared more concrete when asked about specific practices, such as email marketing, targeted advertising, and data deletion. As mentioned earlier, nearly all reported that they had used unsubscribe links within emails. Related to advertising, some participants expected to be able to report a particular advertisement as irrelevant. Half of the participants who mentioned this type of control also mentioned seeing such a control on a social media website, such as Facebook or Twitter. Only a few expected to be able to opt-out of targeted advertising entirely. When asked about choices related to data deletion, some were unaware of deletion controls offered by websites, but about half expected to be able to delete data from their profile and some mentioned being able to delete their entire account. Nearly all participants who mentioned a deletion mechanism stated that they had used such controls in the past.

When asked about privacy controls they wished websites offered, most participants mentioned controls for data sharing and deletion. As P11 stated, *"Well in the ideal world, you should be able to tell the website, look, I'm giving you this information, but don't share it."* A few mentioned wanting to tell websites to not save their information, while a few others desired greater controls over content that is displayed to them, such as recommended articles. More broadly, a few participants expressed a desire for greater transparency about data sharing or existing controls. However, a few others stated that they were satisfied with their current privacy options or could not articulate additional desired control mechanisms.

Formatting and text cause confusion

Another usability issue that made it difficult for participants to interpret choices was poor formatting and explanatory text. Most participants trying to find information about opt-outs for advertising in `coinmarketcap.com`'s privacy policy clicked on the link to install the Google Analytics opt-out browser extension, likely due to the placement of a link in policy text referring to advertisers and the use of cookies. However, the opt-out extension only opts users out of Google's tracking for analytics purposes, and not advertising. Similarly, most participants assigned to `runescape.com` found a page related to data rights, but had difficulty figuring out how to actually request deletion because of the page's format. As seen in Figure 3, removing your personal data appears to be a clickable option. However this is not the case and most were confused about why nothing appeared to happen. The text description provided after a list of data rights directs users to complete a subject access request form, labelled as "Make a Subject Access Request," which is linked after a button labelled "Fix it Fast: Account Settings." Most participants who saw this page incorrectly clicked on the account settings link instead of requesting deletion through emailing the contact provided on the page or the request form, as instructed. The placement of these two links made it unclear which privacy rights listed on the page could be accomplished through each mechanism.[1]

[1]This page on `runescape.com` was updated after our study. The new version partially addresses these issues by reducing the page's

Figure 3. List of data rights available on `runescape.com` which misleadingly seem clickable.

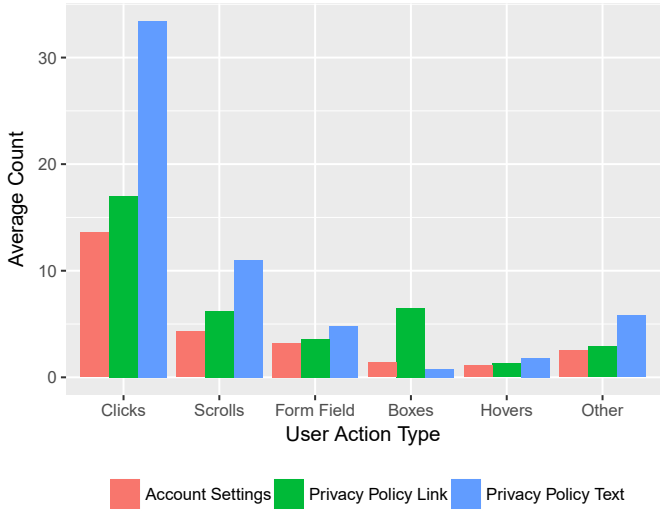

Figure 4. Number of clicks, scrolls, form fields, check boxes, hovers, and other user actions, averaged over all websites, in the participants' interaction with account settings and policy choices.

Conversely, **`colorado.edu`**'s privacy policy contained links to the three advertising opt-out tools in a single paragraph, which led participants to at least see all three tools (even if none actually selected all three, as discussed in the next subsection).

On **`phys.org`** a clear "Manage account" button visible on the landing page of the account settings conveyed the correct interaction path to almost all participants assigned to the website. However, some of the participants who clicked this button and saw the setting to delete the account were unsure whether that mechanism would also delete their data, and navigated away from the page to look for other options. A statement indicating that profile data will be erased permanently was not presented until after clicking the initial delete button. However, once participants saw this confirmation they were assured that the mechanism would accomplish their task.

Physical Action: Using Privacy Choices

Exercising privacy choices required a high level of effort from participants, as measured by the number of actions such as clicks, scrolls, and checkboxes in the interaction path of using a choice mechanism. Certain practices used by the websites in our sample made exercising choices more difficult.

High level of effort exerted in exercising policy choices

Figure 4 displays the number of user actions in participants' interaction path when using privacy choices located in the account settings and privacy policy. Using a choice mechanism in account settings resulted in an average of 26.1 user actions (min: 8, max: 43, sd: 11.5). Interactions using links in the privacy policy had 37.5 actions (min: 11, max: 59, sd: 15.2), on average, and those with text instructions in the policy had 57.6 (min: 18, max: 87, sd: 27.5). While policy links took participants exactly where they needed to go, text instructions were vague and required extra effort to figure out what to do. Furthermore, participants took many more steps than the shortest, ideal path for completing a task. The shortest interaction path for account settings mechanisms would have taken 9 total actions averaged over the three websites, while policy link choices needed 22.3, and policy text required 9.3.

Most participants who used the account settings mechanisms on **`wordpress.com`** or **`phys.org`** said that they were easy to use because of the simplicity of the setting. For example, P6 described the account deletion process on **`phys.org`**: *"It said delete my account which was pretty clear. And then there was this other page that like made it very clear that that's what was going to happen."* Some noted that these mechanisms were easy to find. A few appreciated that, unlike another mechanism they used, the account settings option would be applied right away and did not require a response from the website. Nearly all participants assigned to opt out of emails from **`majorgeeks.com`** also found the mechanism straightforward or easy to use, but most found the setting hard to find.

Participants who were assigned to tasks with privacy choice links or text instructions in the website's privacy policy explicitly mentioned that they found these mechanisms hard to find or that finding them required too much reading. Reactions to the data deletion request form on **`nytimes.com`** were mixed. Most participants disliked being presented with many similar-seeming options related to data processing, only being able to submit one request type at a time, or having to manually select 22 services from a list. However, others reported that the policy was easy to find through the account settings and the form was straightforward to use.

Unsubscribe links within emails were also considered straightforward to find and use. Participants highlighted user-friendly features these pages that they encountered previously or during the study. These included opt-outs that were automatically applied without extra confirmation or entry of their email address, as well as interfaces that allowed users to select emails

text. However, it is still unclear which privacy rights listed can be accomplished by the two mechanisms shown.

from the website they would like to continue to receive (as long as a button to opt-out of all emails was visibly present).

Choices require unnecessary user effort

Some practices used by websites for offering privacy choices place undue burden on users. An example is requiring users to submit written requests, a common practice websites use to offer data deletion [15]. Participants had difficulties articulating such requests. P4, who was trying to opt-out of targeted advertising on **wordpress.com**, drafted a message to customer service that asked *"How can I delete a specific webpage that is contacting me?"* Additionally, a few participants who wrote account deletion or unsubscribe requests did not include all the information the website would need to act on their request, such as the username or email address.

Another practice that complicates opt-out choices for users is offering multiple links to different opt-out tools. The privacy policy for **colorado.edu** contained links to advertising opt-out tools offered by the DAA, NAI, and Google. All participants assigned to this website visited only one or two of the three links. Participants had varying justifications for which links they clicked on. Half selected the DAA and NAI links because they (correctly) believed they would apply to multiple third-parties and not just Google. However, many entities participate in both industry opt-out programs, and participants may not have realized the overlap. Another explained that they chose to click on the Google advertising opt-out because they were already within Google's ecosystem (i.e., using Google Chrome and Gmail) so they thought the opt-out would be more broadly applied, especially if they stayed logged into the Google account. Though Google owns the largest online advertising exchange, using an industry provided opt-out tool may have greater impact on limiting targeted ads.

Simple design flaws also place extra burden on users. For example, on **majorgeeks.com** when a user changes a setting it is not automatically saved; users have to press a "save" button at the bottom of the page. The website also does not provide a warning that there are unsaved changes. A few participants assigned to this website found the correct opt-out setting but did not press "save," resulting in lost changes and the opt-out not being applied. This is an example of a post-completion error [33]. In contrast, a warning reminded a few participants assigned to **wordpress.com** to save their changed settings.

Assessment: Understanding Privacy Choices

Participants expressed skepticism that the privacy choices they use will actually be honored by websites. Websites were also unclear about what happens when such controls are used.

Skepticism of privacy choice effectiveness

During the pre-task interview, participants expressed doubts that data-related controls companies offered actually were effective. A few thought that there was nothing they could do to control ads, or were skeptical that available control mechanisms changed which ads were displayed. As P16 explained, *"It's like the door open/close on the elevator. It's just there to make you feel like you have some power. But I really don't think it does anything."* Others assumed data-sharing agreements between companies precluded opt-outs. P12 explained, *"I think it would be really difficult to like kind of untether them from each other cause I know they have a lot of agreements with each other and stuff like that."* Some expressed skepticism that their data would actually be permanently deleted by a company when requested. As P6 stated, *"I think that I could like go through the motions of deleting the information, but I feel like it might still be there even if I tried to delete it."*

We also noted that skepticism of deletion choices persisted even after participants used deletion mechanisms in the study. A few participants assigned to **phys.org** believed they were simply deactivating their account and that their account data would not actually be deleted by the company. A few others assigned to **nytimes.com** or **runescape.com** were unsure whether or not their data would be fully deleted.

We observed that participants had more confidence in the mechanisms they used to opt-out of email marketing, due in part to prior experience. Almost all participants who used an email opt-out believed that they would eventually stop receiving emails from which they opted out, even if it takes a few days. A few mentioned they might receive a final email to confirm their unsubscribe request.

Confusion about scope of targeted advertising opt-outs

Most participants assigned to use an advertising opt-out had misconceptions about whether the mechanism they used would be effective across different browsers or devices. Some who used cookie based opt-outs on **coinmarketcap.com** or **colorado.edu** were unsure or had misconceptions about whether they would continue seeing targeted ads. Most misconceptions were related to inaccurate mental models of how cookies were stored, with some believing that they were synced to a user's Google profile. Thus they believed that any changes to cookies made using Chrome on a computer would prevent them from seeing targeted ads when they used Chrome on their phone.

DISCUSSION

We conducted an in-lab study with 24 participants to explore the usability and usefulness of privacy controls. Our results highlight several design and policy implications for how websites, particularly those that offer a small number of privacy choices such as those in our sample, should present controls for email marketing, advertising, and deletion. However, further study is needed before these initial findings can be translated to broader policy or design recommendations.

Design Implications

We noted several design decisions that made completing the privacy choice tasks particularly difficult, as well as some that seemed to aid participants. Our findings are especially relevant to controls in user account settings or privacy policies.

Provide unified settings in a standard location

Unifying privacy choices into a single, standard location (perhaps in the form of a dashboard) would likely make these controls easier for users to find. Some participants recognized that many websites have controls in account settings pages and looked for controls there. If the practice of putting privacy choices in account settings was more widely adopted and promoted, it is likely that most users would learn to look there.

However, privacy controls for which a login is not essential should also be available without requiring users to log in or even to have an account.

Privacy controls could also be implemented as an interface within web browsers, which in turn could convey users' choice information to websites in a computer-readable format. This could allow for opting out once for all websites (the idea behind the Do Not Track mechanism), or for all websites that meet certain criteria. It could also save users the effort of finding choice mechanisms on websites and instead allow them to go to the choice menu in their web browser, where they would be provided with available choices that could be exercised through the standard interface.

Supplement with additional paths and in-place controls

Even after unifying choices in one place, websites should still offer multiple paths to those controls so that they are easy to find. Links to privacy controls should be placed anywhere users might look, such as the account settings, privacy policy, and website help pages. For example, all participants assigned to the `nytimes.com` reached the deletion request form in the privacy policy through the account settings, not the link in the website footer mandated by the California Online Privacy Protection Act (CalOPPA). Websites should ensure that if they have multiple links or mechanisms they are consistent with each other and lead to the same results.

Control mechanisms that are offered within the context of how data is used by the website can also supplement unified privacy dashboards. With email marketing, participants in our study were generally aware of unsubscribe links in emails and thought they were easy to find. Similarly, a few participants recalled the ability to control targeted ads on a website by interacting with the corner of an ad.

Reduce effort required to understand and use choice

Websites in our study imposed much of the effort required to exercise privacy choices onto users. It was up to users to distinguish between multiple targeted advertising opt-out tools and figure out how to articulate written deletion requests. For these choices to actually be useful, websites need to place more effort into packaging them into simple settings offered through the website. The mechanisms participants favored the most in our study were toggles or clearly-labelled buttons offered in the account settings. Such settings could automatically place opt-out requests through commonly used industry tools such as those offered by the DAA and NAI, or trigger database queries to remove a user's personal information.

How privacy controls are labelled and organized in a unified privacy dashboard will impact their usability. Our study highlighted that imprecise navigation labels may confuse users. Within a page, controls should be clearly organized and labelled. Websites should conduct user testing with the design of their particular privacy dashboard pages to ensure that people can find the information they need.

Bolster confidence that choices will be honored

Participants in our study were skeptical that privacy choices would actually be honored by websites. Better communication about what exactly a setting does also could help relieve skepticism. For example, `phys.org` stated the time period after which account data would be deleted in the final step of the account deletion process. Websites should also provide confirmation that a choice has been applied after users complete the process. A confirmation message can be displayed within the website itself if the choice is immediately applied. For choices, such as email unsubscribes, that require time to process and complete, at minimum there should be a confirmation message that acknowledges the request and provides a clear estimate of how long it will take to honor the request. For requests, such as those for data deletion, that may take more time before the choice is fully applied, the website should also send a confirmation email.

Public Policy Implications

The recent enactment of comprehensive privacy legislation, such as the GDPR and CCPA, require companies to not only offer privacy choices, but also make them usable. Prior laws, such as the CAN-SPAM Act, included requirements for privacy mechanisms to be clear and conspicuous. Our results indicate that website privacy choices similar to those in our study remain difficult for users to find and use, but that some of these usability requirements are having an impact.

We observed that unsubscribe links within emails had better usability relative to the user account and privacy policy mechanisms we studied. This is likely an effect of CAN-SPAM Act requirements. From our study, it is apparent that unsubscribe links are widely used and that, over time, people have learned to expect these links in the marketing emails they receive. For other regulation to have similar impact, design guidelines for how websites should present privacy choices may be helpful. Guidance on where and how privacy controls should be presented will likely lead to less variation among websites and could allow users to develop consistent expectations. Moreover, future regulation should incorporate the results of usability studies to inform these design guidelines or could require websites to conduct user testing to ensure that choices are useful and usable for consumers.

CONCLUSION

We conducted a 24-participant in-lab usability evaluation of privacy controls related to email marketing, targeted advertising, and data deletion. Our findings highlight the need to better align the location and functionality of choices to user expectations of where to find these choices and how to operate them. Additionally, simple interface changes, including better labeling and use of confirmation messaging, would make choices more useful and increase users' confidence in their effectiveness. Furthermore, the relative success of unsubscribe links mandated by the CAN-SPAM Act suggests that the standardization of choices through regulation could improve the usability of choices.

ACKNOWLEDGMENTS

This project is funded in part by the National Science Foundation (CNS-1330596, CNS-1330214), the Carnegie Corporation of New York, and Innovators Network Foundation. We wish to acknowledge all members of the Usable Privacy Policy Project (www.usableprivacy.org) for their contributions.

REFERENCES

[1] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, and others. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys (CSUR)* 50, 3 (2017), 44.

[2] Terence S Andre, H Rex Hartson, Steven M Belz, and Faith A McCreary. 2001. The User Action Framework: A Reliable Foundation for Usability Engineering Support Tools. *International Journal of Human-Computer Studies* 54, 1 (2001), 107–136.

[3] California State Legislature Website. 2018. SB-1121 California Consumer Privacy Act of 2018. (2018). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

[4] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2019. We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*.

[5] Digital Advertising Alliance. 2009. Self-Regulatory Principles for Online Behavioral Advertising. (July 2009). http://digitaladvertisingalliance.org/principles.

[6] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor Into IoT Device Purchase Behavior. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*.

[7] European Commission. 2018a. Article 29 Data Protection Working Party. Guidelines on Transparency under regulation 2016/679. (2018). http://europa.eu/rapid/press-release_SPEECH-11-461_en.htm.

[8] European Commission. 2018b. EU Data Protection Rules. (2018). https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

[9] Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. 2017. Large-Scale Readability Analysis of Privacy Policies. In *Proceedings of the International Conference on Web Intelligence (WI)*. 18–25.

[10] Federal Trade Commission. 2009. CAN-SPAM Act: A Compliance Guide for Business. (2009). https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

[11] Federal Trade Commission. 2017. Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business. (2017). https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

[12] Stacia Garlach and Daniel Suthers. 2018. 'I'm supposed to see that?'AdChoices Usability in the Mobile Environment. In *Proceedings of the Hawaii International Conference on System Sciences (HICSS)*.

[13] Global Privacy Enforcement Network. 2017. GPEN Sweep 2017: User Controls over Personal information. (2017). https://www.privacyenforcement.net/system/files/2017%20GPEN%20Sweep%20-%20International%20Report_0.pdf.

[14] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*.

[15] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2019. An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.

[16] Jovanni Hernandez, Akshay Jagadeesh, and Jonathan Mayer. 2011. Tracking the Trackers: The AdChoices Icon. (2011). http://cyberlaw.stanford.edu/blog/2011/08/tracking-trackers-adchoices-icon.

[17] IAB Europe. 2011. EU Framework for Online Behavioural Advertising. (2011). https://www.edaa.eu/wp-content/uploads/2012/10/2013-11-11-IAB-Europe-OBA-Framework_.pdf.

[18] IAB Europe. 2019. GDPR Transparency and Consent Framework. (2019). https://iabtechlab.com/standards/gdpr-transparency-and-consent-framework/.

[19] JustDelete.me. 2019. A directory of direct links to delete your account from web services. (2019). https://justdeleteme.xyz.

[20] Saranga Komanduri, Richard Shay, Greg Norcie, and Blase Ur. 2011. AdChoices? Compliance with Online Behavioral Advertising Notice and Choice Requirements. *A Journal of Law and Policy for the Information Society* 7 (2011).

[21] Pedro Giovanni Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu. 2012. What Do Online Behavioral Advertising Privacy Disclosures Communicate to Users?. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*.

[22] Thomas Linden, Hamza Harkous, and Kassem Fawaz. 2018. The Privacy Policy Landscape After the GDPR. *arXiv:1809.08396* (2018).

[23] Mary Madden and Lee Rainie. 2015. Americans' Attitudes About Privacy, Security and Surveillance. (2015).

[24] Arunesh Mathur, Jessica Vitak, Arvind Narayanan, and Marshini Chetty. 2018. Characterizing the use of browser-based blocking extensions to prevent online tracking. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.

[25] Jonathan R Mayer and John C Mitchell. 2012. Third-Party Web Tracking: Policy and Technology. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*.

[26] Aleecia M McDonald and Lorrie Faith Cranor. 2010. Americans' Attitudes About Internet Behavioral Advertising Practices. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*.

[27] William Melicher, Mahmood Sharif, Joshua Tan, Lujo Bauer, Mihai Christodorescu, and Pedro Giovanni Leon. 2016. (Do Not) Track Me Sometimes: Users' Contextual Preferences for Web Tracking. *Proceedings on Privacy Enhancing Technologies* 2016, 2 (2016), 135–154.

[28] Michael Morgan, Daniel Gottlieb, Matthew Cin, Jonathan Ende, Amy Pimentel, and Li Wang. 2018. California Enacts a Groundbreaking New Privacy Law. (2018). https://www.mwe.com/en/thought-leadership/publications/2018/06/california-enacts-groundbreaking-new-privacy-law.

[29] Ambar Murillo, Andreas Kramm, Sebastian Schnorf, and Alexander De Luca. 2018. "If I press delete, it's gone" - User Understanding of Online Data Deletion and Expiration. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)* (2018).

[30] Network Advertising Initiative. 2018. NAI Code of Conduct. (2018). https://www.networkadvertising.org/sites/default/files/nai_code2018.pdf.

[31] Nielsen Norman Group. 2018. Top 10 Design Mistakes in the Unsubscribe Experience. (2018). https://www.nngroup.com/articles/unsubscribe-mistakes/.

[32] Donald A. Norman. 1986. Cognitive Engineering. In *User Centered System Design: New Perspectives on Human-Computer Interaction*. Lawrence Erlbaum Associates, 31–61.

[33] Donald A. Norman. 1990. *The Design of Everyday Things*. Doubleday.

[34] Norwegian Consumer Council. 2018. Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy. (2018). https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[35] Online Trust Alliance. 2018. Email Marketing & Unsubscribe Audit. (2018). https://www.internetsociety.org/resources/ota/2018/2018-email-marketing-unsubscribe-audit/.

[36] Enric Pujol, Oliver Hohlfeld, and Anja Feldmann. 2015. Annoyed Users: Ads and Ad-Block Usage in the Wild. In *Proceedings of the Internet Measurement Conference*.

[37] Iskander Sanchez-Rola, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, and Igor Santos. 2019. Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control. In *Proceedings of the ACM Asia Conference on Computer and Communications Security*.

[38] Florian Schaub, Aditya Marella, Pranshu Kalvani, Blase Ur, Chao Pan, Emily Forney, and Lorrie Faith Cranor. 2016. Watching Them Watching Me: Browser Extensions' Impact on User Privacy Awareness and Concern. In *Proceedings of NDSS Workshop on Usable Security (USEC)*.

[39] Fatemeh Shirazi and Melanie Volkamer. 2014. What Deters Jane from Preventing Identification and Tracking on the Web?. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*.

[40] United States Congress. 1999. S.900 - Gramm-Leach-Bliley Act. (1999). https://www.congress.gov/bill/106th-congress/senate-bill/00900.

[41] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.

[42] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of Conference on Computer and Communications Security (CCS)*.

[43] Ari Ezra Waldman. 2019. There is No Privacy Paradox: How Cognitive Biases and Design Dark Patterns Affect Online Disclosure. *Current Opinion in Psychology* (2019).